

Matthew Franklin Jaksa (State Bar No. 248072)
HOLME ROBERTS & OWEN LLP
560 Mission Street, 25th Floor
San Francisco, CA 94105-2994
Telephone: (415) 268-2000
Facsimile: (415) 268-1999
E-mail: matt.jaksa@hro.com

Attorney for Plaintiffs
VIRGIN RECORDS AMERICA, INC.;
INTERSCOPE RECORDS; SONY BMG
MUSIC ENTERTAINMENT; CAPITOL
RECORDS, INC.; UMG RECORDINGS, INC.;
and WARNER BROS. RECORDS INC.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

VIRGIN RECORDS AMERICA, INC., a California
corporation; INTERSCOPE RECORDS, a
California general partnership; SONY BMG
MUSIC ENTERTAINMENT, a Delaware general
partnership; CAPITOL RECORDS, INC., a
Delaware corporation; UMG RECORDINGS, INC.,
a Delaware corporation; and WARNER BROS.
RECORDS INC., a Delaware corporation,,

Plaintiff,

v.

JOHN DOE,

Defendant.

FILED

FEB 28 2008

RICHARD W. WIEKING
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

BZ

Case No. **CV 08 1191**

**DECLARATION OF CARLOS
LINARES IN SUPPORT OF *EX PARTE*
APPLICATION FOR LEAVE TO
TAKE IMMEDIATE DISCOVERY**

**DECLARATION OF CARLOS LINARES IN
SUPPORT OF *EX PARTE* APPLICATION FOR LEAVE
TO TAKE IMMEDIATE DISCOVERY**

ORIGINAL

1
2 I, Carlos Linares, have personal knowledge of the facts stated below and, under penalty
3 of perjury, hereby declare:

4 1. I am Vice President, Anti-Piracy Legal Affairs for the Recording Industry
5 Association of America, Inc. ("RIAA"), where I have been employed for over six years. My office is
6 located at 1025 F Street, N.W., 10th Floor, Washington, DC 20004. I submit this Declaration in
7 support of Plaintiffs' *Ex Parte* Application for Leave to Take Immediate Discovery.

8 2. As Vice President, Anti-Piracy Legal Affairs, I am responsible for evaluating
9 and contributing to online strategies for the RIAA, including oversight of the investigations into online
10 infringement of copyrighted sound recordings. As such, this Declaration is based on my personal
11 knowledge, and if called upon to do so, I would be prepared to testify as to its truth and accuracy.

12 **The RIAA's Role in Protecting Its Member Recording Industry Companies From Copyright**
13 **Infringement**

14 3. The RIAA is a not-for-profit trade association whose member record companies
15 create, manufacture, and/or distribute approximately ninety percent of all legitimate sound recordings
16 produced and sold in the United States. The RIAA's member record companies comprise the most
17 vibrant national music industry in the world. A critical part of the RIAA's mission is to assist its
18 member companies in protecting their intellectual property in the United States and in fighting against
19 online and other forms of piracy. All of the Plaintiffs in this action are members of the RIAA.

20 4. As part of that process, the RIAA, on behalf of its members, retains a variety of
21 services from outside vendors to assist with its investigation of the unauthorized reproduction and
22 distribution of copyrighted sound recordings online.

23 **The Internet and Music Piracy**

24 5. The Internet is a vast collection of interconnected computers and computer
25 networks that communicate with each other. It allows hundreds of millions of people around the world
26 to communicate freely and easily and to exchange ideas and information, including academic research,
27

1 literary works, financial data, music, movies, graphics, and an unending and ever-changing array of
2 other data. Unfortunately, the Internet also has afforded opportunities for the wide-scale piracy of
3 copyrighted sound recordings and musical compositions. Once a sound recording has been
4 transformed into an unsecured digital format, it can be copied further and distributed an unlimited
5 number of times over the Internet, without significant degradation in sound quality.

6 6. Much of the unlawful distribution of copyrighted sound recordings over the
7 Internet occurs via “peer-to-peer” (“P2P”) file copying networks or so-called online media distribution
8 systems. The most notorious example of such a system was Napster, which was enjoined by a federal
9 court. Notwithstanding the court’s decision enjoining Napster, similar online media distribution
10 systems emerged and attempted to capitalize on the growing illegal market that Napster fostered.
11 These include KaZaA, eDonkey, iMesh, Ares, BitTorrent, DirectConnect, and Gnutella, among others.
12 To this day, some P2P networks continue to operate and to facilitate widespread copyright piracy. At
13 any given moment, millions of people illegally use online media distribution systems to upload or
14 download copyrighted material.

15 7. P2P networks, at least in their most popular form, refer to computer systems or
16 processes that enable Internet users to: (1) make files (including audio recordings) stored on a
17 computer available for copying by other users; (2) search for files stored on other users’ computers;
18 and (3) transfer exact copies of files from one computer to another via the Internet. P2P networks
19 enable users who otherwise would have no connection with, or knowledge of, each other to offer to
20 each other for distribution and copying files off of their personal computers, to provide a sophisticated
21 search mechanism by which users can locate these files for downloading, and to provide a means of
22 effecting downloads.

23 8. The major record companies generally have not authorized their copyrighted
24 sound recordings to be copied or distributed in unsecured formats by means of P2P networks. Thus,
25 the vast majority of the content that is copied and distributed on P2P networks is unauthorized by the
26 copyright owner – that is, the distribution violates the copyright laws.

1 9. The scope of online piracy of copyrighted works cannot be underestimated. The
2 RIAA member companies lose significant revenues on an annual basis due to the millions of
3 unauthorized downloads and uploads of well-known recordings that are distributed on P2P networks
4 by infringers who, in virtually all cases, have the ability to maintain their anonymity to all but the
5 Internet Service Provider ("ISP") they use to supply them with access to the Internet.

6 10. The persons who commit infringements by using the P2P networks are, by and
7 large, anonymous to Plaintiffs. A person who logs on to a P2P network is free to use any alias (or
8 computer name) whatsoever, without revealing his or her true identity to other users. Thus, Plaintiffs
9 can observe the infringement occurring on the Internet, but do not know the true names or mailing
10 addresses of those individuals who are committing the infringement.

11 **The RIAA's Identification of Copyright Infringers**

12
13 11. In order to assist its members in combating copyright piracy, the RIAA retained
14 a third-party investigator, MediaSentry, Inc. ("MediaSentry"), to conduct searches of the Internet, as
15 well as file-copying services, for infringing copies of sound recordings whose copyrights are owned by
16 RIAA members. A search can be as simple as logging onto a P2P network and examining what files
17 are being offered by others logged onto the network. In gathering evidence of copyright infringement,
18 MediaSentry uses the same functionalities that are built into P2P programs that any user of the
19 software can use on the network.

20 12. Users of P2P networks who distribute files over a network can be identified by
21 using Internet Protocol ("IP") addresses because the unique IP address of the computer offering the
22 files for distribution can be captured by another user during a search or a file transfer. Users of P2P
23 networks can be identified by their IP addresses because each computer or network device (such as a
24 router) that connects to a P2P network must have a unique IP address within the Internet to deliver files
25 from one computer or network device to another. Two computers cannot effectively function if they
26 are connected to the Internet with the same IP address at the same time. This is analogous to the
27 telephone system where each location has a unique number. For example, in a particular home, there

1 may be three or four different telephones, but only one call can be placed at a time to or from that
2 home. Each computer or network device is connected to a network that is administered by an
3 organization like a business, ISP, college, or university. Each network, in turn, is analogous to an area
4 code. The network provider maintains a log of IP address allocations. An IP address can be associated
5 with an organization such as an ISP, business, college, or university, and that organization can identify
6 the P2P network user associated with the specified IP address.

7 13. MediaSentry finds individuals using P2P networks to share music files over the
8 Internet. Just as any other user on the same P2P networks as these individuals would be able to do,
9 MediaSentry is able to detect the infringement of copyrighted works and identify the users' IP
10 addresses because the P2P software being used by those individuals has file-sharing features enabled.

11 14. For each suspected infringer, MediaSentry downloads a number of the music
12 files that the individual is offering to other users on the P2P network. Those music files for each such
13 individual are listed in Exhibit A to the Complaint. MediaSentry assigns an identification number to
14 each individual for which it detects copyright infringement and gathers additional evidence for each
15 individual, such as metadata accompanying each file being disseminated that demonstrates that the
16 user is engaged in copyright infringement. That evidence includes download data files that show for
17 each music file the source IP address, user logs that include a complete listing of all files in the
18 individual's share folder at the time, and additional data that track the movement of the files through
19 the Internet.

20 15. After MediaSentry collects the evidence of infringement, the RIAA engages in a
21 painstaking process to verify whether each individual was infringing. That process relies on human
22 review of evidence supporting the allegation of infringement. For each suspected infringer, the RIAA
23 reviews a listing of the music files that the user has offered for download by others from his or her
24 computer in order to determine whether they appear to be copyrighted sound recordings. The RIAA
25 also listens to the downloaded music files from these users in order to confirm that they are, indeed,
26 illegal copies of sound recordings whose copyrights are owned by RIAA members. Exhibit A to the
27

1 Complaint lists the details of these downloaded music files. In my role as Vice President, Anti-Piracy,
2 I provide oversight over the review of the lists contained in Exhibit A to the Complaint and hereby
3 attest to the veracity of those lists. The RIAA also reviews the other evidence collected by
4 MediaSentry.

5 **The Subpoena Process to Identify Copyright Infringers**

6
7 16. The RIAA frequently has used the subpoena processes of Federal Rule of Civil
8 Procedure 45 and the Digital Millennium Copyright Act ("DMCA") to obtain the names of infringers
9 from ISPs. The RIAA typically has included in their subpoenas to ISPs an IP address and a date and
10 time on which the RIAA, through its agent, MediaSentry, observed use of the IP address in connection
11 with allegedly infringing activity. In some instances, providing the IP address alone to the ISP has
12 been enough to enable the ISP to identify the infringer. Providing the date and time further assists
13 some ISPs in identifying infringers, especially ISPs that use "dynamic IP addressing" such that a single
14 computer may be assigned different IP addresses at different times, including, for example, each time it
15 logs into the Internet.¹ Once provided with the IP address, plus the date and time of the infringing
16 activity, the infringer's ISP quickly and easily can identify the computer from which the infringement
17 occurred (and the name and address of the subscriber that controls that computer), sometimes within a
18 matter of minutes.

19 17. Since 1998, the RIAA and others have used subpoenas thousands of times to
20 learn the names, addresses, telephone numbers, and e-mail addresses of infringers for the purpose of
21 bringing legal actions against those infringers. During a recent litigation with Verizon (an ISP)
22 relating to the DMCA subpoena process, Verizon conceded that, as an alternative to the DMCA
23 process, Plaintiffs could file "Doe" lawsuits and issue Rule 45 subpoenas to ISPs to obtain the true
24 identities of infringing subscribers.

25
26 ¹ ISPs own or are assigned certain blocks or ranges of IP addresses. An ISP assigns a particular
27 IP address in its block or range to a subscriber when that subscriber goes "online."

The RIAA's Identification of the Infringers in This Case

18. In the ordinary course of investigating online copyright infringement, the RIAA became aware that Defendant was offering files for download on various P2P networks. The user-defined author and title of the files offered for download by Defendant suggested that many were copyrighted sound recordings being disseminated without the authorization of the copyright owners. The RIAA downloaded and listened to a representative sample of the music files being offered for download by Defendant and was able to confirm that the files Defendant was offering for distribution were illegal copies of sound recordings whose copyrights are owned by RIAA members. The RIAA also recorded the time and date at which the infringing activity was observed and the IP address assigned to Defendant at the time. See Complaint Exhibit A. The RIAA could not, however, determine the physical location of the users or their identities. The RIAA could determine that Defendant was using Stanford University internet service to distribute and make available for distribution the copyrighted files.

19. The RIAA also has collected a list of the files Defendant has made available for distribution to the public. This list shows hundreds of files, many of which are sound recording (MP3) files that are owned by, or exclusively licensed to, Plaintiffs. Because of the voluminous nature of the list, and in an effort not to overburden the Court with paper, I have not attached to this Declaration that list. Such list will be made available to the Court upon request. Exhibit A to the Complaint includes the username of the infringer if that was available, the identification number assigned by MediaSentry for Defendant, and the number of audio files that were being shared by Defendant at the time that the RIAA's agent, MediaSentry, observed the infringing activity.

The Importance of Expedited Discovery in This Case

20. Obtaining the identity of copyright infringers on an expedited basis is critical to stopping the piracy of the RIAA members' copyrighted works.

21. First, every day that copyrighted material is disseminated without the authorization of the copyright owner, the copyright owner is economically harmed. Prompt

1 identification of infringers is necessary in order for copyright owners to take quick action to stop
2 unlawful dissemination of their works and minimize their economic losses.

3 22. Second, infringement often occurs with respect to sound recordings that have
4 not yet been distributed publicly. Such infringement inflicts great harm on the initial market for new
5 works. New recordings generally earn a significant portion of their revenue when they are first
6 released, and copyright piracy during a recording's pre-release or early release period therefore
7 deprives copyright owners of an important opportunity to reap the benefits of their labor.

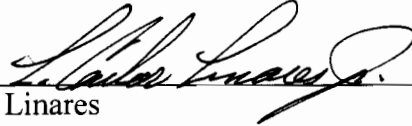
8 23. Third, without expedited discovery, Plaintiffs have no way of serving Defendant
9 with the complaint and summons in this case. Plaintiffs do not have Defendant's name or address, nor
10 do they have an e-mail address for Defendant.

11 24. Fourth, and perhaps most critically, ISPs have different policies pertaining to the
12 length of time they preserve "logs" which identify their users. ISPs keep log files of their user
13 activities for only limited periods of time – which can range from as short as a few days, to a few
14 months – before erasing the data they contain. If an ISP does not respond expeditiously to a discovery
15 request, the identification information in the ISP's logs may be erased, making it impossible for the
16 ISP to determine the identity of the infringer and eliminating the copyright owner's ability to take
17 action to stop the infringement.

18 *[Remainder of page intentionally left blank.]*
19
20
21
22
23
24
25
26
27
28

1 I declare under penalty of perjury under the laws of the United States that the foregoing is true
2 and correct.

3 Executed on February 2, 2008 in Washington, D.C.
4

5 
6 Carlos Linares